DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **25 Oct 12**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Special Interoperability Test Certification of the NetApp FAS3170 with DATA ONTAP Software Release (SR) 7.3.6

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (f), see Enclosure

1. References (a) and (b) establish Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The NetApp FAS3170 with DATA ONTAP with SR 7.3.6, hereinafter referred to as the System Under Test (SUT), meets all the critical interoperability requirements for a Data Storage Controller and is certified for joint use within the Defense Information System Network (DISN). The certification status of the SUT will be verified during operational deployment. Any new discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of Defense Information Systems Agency (DISA) via a vendor Plan of Action and Milestones which addresses all new critical Test Discrepancy Reports within 120 days of identification. Testing was conducted using product requirements derived from the Unified Capabilities Requirements (UCR), Reference (c), and test procedures, Reference (d). No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that affect interoperability, but no later than 17 August 2015, three years from the date of the Unified Capabilities Approved Products List memorandum.

3. The extension of this certification is based upon Desktop Review (DTR) 1. The original certification is based on interoperability testing conducted by Telecommunication Systems Security Assessment Program (TSSAP), review of the vendor's Letters of Compliance (LoC), and TSSAP Information Assurance (IA) Certification Authority (CA) approval of the IA configuration, and documented in Reference (e). Interoperability testing was conducted by TSSAP from 8 through 11 November 2011, 29 November through 2 December 2011, and 12 through 16 December 2011. Review of the vendor's LoC was completed on 7 January 2012. The DISA CA has reviewed the IA Assessment Report for the SUT, Reference (f), and based on the findings in the report provided a positive recommendation on 15 March 2012. This DTR was requested to include the additional model numbers listed in Table 1. The additional model numbers use the same software and similar hardware as the SUT and JITC determined through analysis they are identical for interoperability certification purposes. Therefore, JITC approves

this DTR. The IA posture has not changed. Therefore, the original IA approval applies to this DTR.

Table 1. UC APL Product Summary

Component[1]	Release
FAS6030	Data ONTAP Release 7.3.6
GF980	Data ONTAP Release 7.3.6
FAS980	Data ONTAP Release 7.3.6
FAS6070	Data ONTAP Release 7.3.6
FAS960	Data ONTAP Release 7.3.6
GF960	Data ONTAP Release 7.3.6
FAS6080	Data ONTAP Release 7.3.6
FAS6040	Data ONTAP Release 7.3.6
FAS3050	Data ONTAP Release 7.3.6
FAS3070	Data ONTAP Release 7.3.6
V3070	Data ONTAP Release 7.3.6
FAS920	Data ONTAP Release 7.3.6
FAS940	Data ONTAP Release 7.3.6
GF920	Data ONTAP Release 7.3.6
GF940	Data ONTAP Release 7.3.6
R200	Data ONTAP Release 7.3.6
FAS3020	Data ONTAP Release 7.3.6
V3020	Data ONTAP Release 7.3.6
FAS3040	Data ONTAP Release 7.3.6
V3040	Data ONTAP Release 7.3.6
FAS3270 with Expanded I/O[2]	Data ONTAP Release 7.3.6
FAS3270	Data ONTAP Release 7.3.6
FAS3240 with Expanded I/O[2]	Data ONTAP Release 7.3.6
FAS3240	Data ONTAP Release 7.3.6
FAS3210	Data ONTAP Release 7.3.6
FAS3140	Data ONTAP Release 7.3.6
FAS3160	Data ONTAP Release 7.3.6
V3210	Data ONTAP Release 7.3.6
V3240 with Expanded I/O[2]	Data ONTAP Release 7.3.6
V3270 with Expanded I/O[2]	Data ONTAP Release 7.3.6
FAS2050	Data ONTAP Release 7.3.6
FAS250	Data ONTAP Release 7.3.6
FAS270	Data ONTAP Release 7.3.6
GF270C	Data ONTAP Release 7.3.6
FAS2020	Data ONTAP Release 7.3.6
FAS2050A	Data ONTAP Release 7.3.6
FAS2040	Data ONTAP Release 7.3.6

NOTE:
1. The products listed in this table are certified by JITC analysis because they employ the same software and similar hardware as the SUT.
2. Expanded I/O products have a dual enclosure and 12 PCIe expansion slots instead of a single enclosure and 4 PCIe expansion slots.

LEGEND:

APL	Approved Products List	SUT	System Under Test
I/O	Input/Output	TSSAP	Telecommunication Systems Security Assessment Program
JITC	Joint Interoperability Test Command	UC	Unified Capabilities
PCIe	Peripheral Component Interconnect Express		

4. The interface, Capability Requirements (CR) and Functional Requirements (FR), and component status of the SUT are listed in Tables 2 and 3. The threshold CR/FRs for security devices are established by Section 5.10 of Reference (c) and were used to evaluate the interoperability of the SUT.

Table 2. SUT Interface Interoperability Status

Interface	Critical	UCR Reference	Threshold CR/FR[1]	Status	Remarks
Network Attached Storage (NAS)					
10Base-X	Yes	5.10.4.3	1-11	Certified	The SUT met all critical CRs and FRs for the interface.
100Base-X	Yes	5.10.4.3	1-11	Certified	The SUT met all critical CRs and FRs for the interface.
Gigabit Ethernet (GbE)	Yes	5.10.4.1	1-11	Certified	The SUT met all critical CRs and FRs for the interface.
10 GbE	Yes	5.10.4.1	1-11	Certified	The SUT met all critical CRs and FRs for the interface.
Storage Array Network (SAN)					
Fibre Channel (FC)	No	5.10.5.1	1-11	Not Tested[2]	This interface is supported by the SUT but was not tested and is not certified for use.
FC Protocol (FCP)	No	5.10.5.1	1-11	Not Tested[2]	This interface is supported by the SUT but was not tested and is not certified for use.
Converged Network Adapter (CNA)					
10 GbE	No	5.10.6.1	1-11	Not Tested	Not applicable.

NOTES:
1. CR/FR requirements are contained in Table 3. CR/FR numbers represent a roll-up of UCR requirements
2. The requirement is not critical, was not tested, and therefore is not certified for use.

LEGEND:

CNA	Converged Network Adaptor	ID	Identification
CR	Capability Requirement	NAS	Network Attached Storage
FC	Fibre Channel	SAN	Storage Array Network
FCP	FC Protocol	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements
GbE	Gigabit Ethernet		

Table 3. SUT CRs and FRs Status

CR/FR ID	Capability/Function	Applicability	UCR References	Status
1	**Storage System Requirements**			
	Redundant Array of Independent Disks (RAID)	Required	5.10.2.1	Met
	Availability	Required	5.10.2.2	Met[1]
	Management Control	Required	5.10.2.3	Met
	Data Storage Replication	Required	5.10.2.4	Met
	Data Storage Backup	Required	5.10.2.4.1	Met
	Replication	Required	5.10.2.4.2	Met
	Disaster Recovery (DR)	Required	5.10.2.4.3	Met
	Configuration Modes	Conditional	5.10.2.5	Met

Table 3. SUT CRs and FRs Status (continued)

CR/FR ID	Capability/Function	Applicability	UCR References	Status
2	**Storage Protocol Requirements**			
	Network File System (NFSv3)	Required	5.10.3.1	Met
	Network File System (NFSv4)	Conditional	5.10.3.2	Met
	Network File System (NFSv4.1)	Conditional	5.10.3.3	Not Tested
	Common Internet File System (CIFSv1.0)	Required	5.10.3.4	Met
	Common Internet File System (CIFSv2.0)	Conditional	5.10.3.5	Met
	Internet Small Computer System Interface (iSCSI)	Conditional	5.10.3.6	Met
	Fibre Channel (FC) Protocol	Conditional	5.10.3.7	Not Tested[2]
	Fibre Channel over Ethernet (FCoE)	Conditional	5.10.3.8	Not Tested[2]
	HTTPS Server	Conditional	5.10.3.9	Not Tested[3]
	SSHv2 or SSL Implementation	Required	5.10.3.10	Met
	Web-based Distributed Authoring and Versioning (WebDAV)	Conditional	5.10.3.11	Not Tested[3]
	Representational State Transfer (REST)	Conditional	5.10.3.12	Not Tested[4]
	Cloud Data Management Interface (CDMI)	Conditional	5.10.3.13	Not Tested[4]
	Global Name Space (GNS) functionality	Required	5.10.3.14	Not Met[5]
3	**Network Attached Storage (NAS) Interface Requirements**			
	Gigabit Ethernet (GbE) and 10 GbE Services	Required	5.10.4.1	Met
	Provision, Monitor and Detect Faults, and Restore Ethernet	Required	5.10.4.2	Met
	SSHv2, SSL,HTTPS, and SNMPv3 Protocols	Required	5.10.4.3	Met
	Auto-sensing, Auto-detecting and Auto-configuring	Required	5.10.4.4	Met
	Ethernet Services and Logical Link IWF	Required	5.10.4.5	Met[1]
	Ethernet Service Requirements	Required	5.10.4.6	Met
	VLAN Requirements	Required	5.10.4.7	Met
	Link Aggregation	Required	5.10.4.8	Met
	Link Layer Discovery Protocol (LLDP)	Required	5.10.4.9	Partially Met[6]
4	**Storage Array Network (SAN) Interface Requirements**			
	Fiber Channel (FC) Physical Interfaces	Conditional	5.10.5.1	Not Tested[2]
5	**Converged Network Adapter (CAN) Interface Requirements**			
	FCoE Services	Conditional	5.10.6.1	Not Tested[2]
	Data Center Bridging (DCB) Table 5.10.6-1	Conditional	5.10.6.2	Not Tested[2]
6	**IP Networking Requirements**			
	IPv6 Requirements as defined in Section 5.3.5.5	Required	5.10.7.1	Met[1,7]
	Replication (mirroring) Session Traffic Per Table 5.10.7-1	Required	5.10.7.3	Met[1]
	Congestion Control	Required	5.10.7.4	Met[1]
7	**Name Services Requirements**			
	Lightweight Directory Access Protocol (LDAP)	Required	5.10.8.1	Met[7]
	Kerberos Authentication	Required	5.10.8.2	Met
	Domain Name System (DNS) Functionality	Required	5.10.8.3	Met
	DNS Load Balancing	Required	5.10.8.4	Met
	Network Information Service (NIS) Functionality	Required	5.10.8.5	Met[7]
	NIS Netgroups Functionality	Required	5.10.8.6	Met[7]
	NetBIOS over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS)	Conditional	5.10.8.7	Met
	Internet Storage Name Service (iSNS) Functionality	Required	5.10.8.8	Met[1]
	FC Name and Zone Service	Required	5.10.8.9	Not Tested[8]

Table 3. SUT CRs and FRs Status (continued)

CR/FR ID	Capability/Function	Applicability	UCR Reference	Status
8	**Security Services Requirements**			
	IPSec	Conditional	5.10.9.1	Met[1]
	Encapsulating Security Payload (ESP)	Conditional	5.10.9.2	Met[1]
	Internet Key Exchange version 2 (IKEv2)	Conditional	5.10.9.3	Met[1]
	The Packet Filter Service	Conditional	5.10.9.4	Not Tested[2]
	DoD Host-Based Security System (HBSS) Software	Conditional	5.10.9.5	Not Tested[2]
	Data Encryption	Required	5.10.9.6	Met[7]
	STIGs Compliance	Required	5.10.9.7	Met[7]
9	**Interoperability Requirements**			
	IP ASLAN and DISN WAN Networks	Required	5.10.10.1	Met
	Application Programming Interface (API)	Required	5.10.10.2	Met
10	**Class of Service (CoS) and Quality of Service (QoS) Requirements**			
	Layer 2 CoS and QoS Markings	Required	5.10.11.1	Not Met[9]
	Layer 3 CoS and QoS Markings	Required	5.10.11.2	Met
11	**Virtualization Requirements**			
	Virtualized Data Storage Controller (vDSC) Functionality	Conditional	5.10.12.1	Not Tested
	Private Networking Domains (PNDs)	Conditional	5.10.12.2	Not Tested
	Individual Command Line Interface (CLI)	Conditional	5.10.12.3	Not Tested
	API Commands	Conditional	5.10.12.4	Not Tested
	GNS	Conditional	5.10.12.5	Not Tested

NOTES:
1. This UCR Requirement is met by the vendor's letter of compliance (LoC).
2. This requirement is conditional, was not tested, and therefore is not certified for use.
3. The SUT has no WEB Server functionality in the tested configuration and therefore is not certified for WebDAV.
4. Representational State Transfer (REST) for distributed hypermedia systems and Cloud-Based functionalities are not included in this SUT and therefore the SUT is not certified for REST or CDMI.
5. Global Name Space is not natively supported on the Data ONTAP filer for Version 7.3.6. On 4 May 2012, DISA adjudicated this as minor with a condition of fielding (COF) and POA&M. The COF is that a secondary component like a load balancer with global load balancing capability may be used. The POA&M is the software release of Data ONTAP version 8.2, which is projected to occur in third quarter 2013, with Global Name Space functionality included.
6. The Ethernet services of the SUT only provide LLDP via the Cisco Discovery Protocol (CDP) in lieu of LLDP, which was adjudicated as a minor issue. On 28 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from "required" to "conditional" in a future version of the UCR and also because the implementation of discovery protocol (LLDP or CDP) is dependent upon the infrastructure that the DSC connects to. Therefore, the procurement requirements for DSC should specify the needed discovery protocol.
7. The test results for this requirement were published in a separate report. See Reference (f).
8. On 12 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from "required" to "conditional" to be consistent with all other fiber channel requirements for a DSC. This requirement will change to conditional in UCR 2013.
9. On 12 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from "required" to "conditional" to align on layer 3 queuing for QoS and no longer requiring layer 2 CoS marking. This requirement will change to conditional in UCR 2013.

Table 3. SUT CRs and FRs Status (continued)

LEGEND:

ASLAN	Assured Service Local Area Network
API	Application Programming Interface
CDMI	Cloud Data Management Interface
CDP	Cisco Discovery Protocol
CLI	Individual Command Line Interface
CNA	Converged Network Adaptor
CoS	Class Of Service
CR	Capability Requirement
DCB	Data Center Bridging
DISN	Defense Information Systems Network
DNS	Domain Name System
DoD	Department Of Defense
DR	Disaster Recovery
DSC	Data Storage Controller
ESP	Encapsulating Security Payload
FC	Fibre Channel
FCP	FC Protocol
FCoE	FC Over Ethernet
FC	Fibre Channel
FCP	FC Protocol
FR	Functional Requirement
GbE	Gigabit Ethernet
GNS	Global Name Space
HBSS	Host-Based Security System
HTTPS	Hypertext Transport Protocol Secure
ID	Identification
IKEv2	Internet Key Exchange Version 2
IP	Internet Protocol
IPSEC	Internet Protocol Security
IPv6	Internet Protocol Version 6
iSCSI	Internet Small Computer System Interface
iSNS	Internet Storage Name Service
IWF	Interworking Function
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
NAS	Network Attached Storage
NBT	NetBIOS Over TCP/IP
NIS	Network Information Service
PND	Private Networking Domains
POA&M	Plan of Action and Milestones
QoS	Quality Of Service
RAID	Redundant Array Of Independent Disks
REST	Representational State Transfer
SAN	Storage Array Network
SNMPv3	Simple Network Management Protocol Version 3
SSHv2	Secure Shell Version 2
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
TCP/IP	Transmission Control Protocol/Internet Protocol
UCR	Unified Capabilities Requirements
vDSC	Virtualized Data Storage Controller
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WebDAV	Web-Based Distributed Authoring And Versioning
WINS	Windows Internet Name Service

5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi. All associated data is available on the Defense Information Systems Agency Unified Capability Coordination Office (UCCO) website located at https://aplits.disa.mil.

6. The testing point of contact is Ryan Bradshaw, TSSAP, commercial (210) 925-6900 or DSN 945-6900; e-mail address is ryan.bradshaw.3@us.af.mil. The JITC certification point of contact is Anita Mananquil, commercial (520) 538-5164 or DSN (312) 879-5164; e-mail address is anita.mananquil.civ@mail.mil. JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-1298. The Unified Capabilities Connection Office tracking number is 1111701.

FOR THE COMMANDER:

Enclosure a/s

for BRADLEY A. CLARK
Acting Chief
Battlespace Communications Portfolio

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
USD(AT&L)
ISG Secretariat, DISA, JTA
U.S. Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division
US Coast Guard, CG-64
DISA/TEMC
DIA, Office of the Acquisition Executive
NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V
HQUSAISEC, AMSEL-IE-IS
UCCO

ADDITIONAL REFERENCES

(c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 3," September 2011
(d) Joint Interoperability Test Command, "Storage Device Test Plan," Draft
(e) Joint Interoperability Test Command, Memo, JTE, "Special Interoperability Test Certification of the NetApp FAS3170 with DATA ONTAP Software Release (SR) 7.3.6," 5 October 2012
(f) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of NetApp, FAS3170 Data Storage Controller with Rel. 7.3.6 (TN 1111701)," 12 March 2012